Analysis of Data Hiding Algorithms

[1]E.Divya, [2]P.Rajkumar
[1,2]Department of ECE, Nehru College of Engineering and Research Centre,
Thrissur, India

Abstract—Steganography or concealed writing refers to the technique of hiding secret information. There are many covers available to hide objects.This paper describes the basic steganographic data hiding technques. The paper also compares the spatial and transform domain techniques by comparing their peak signal to noise ratio and computation time.

Index Terms—LSB, DCT, DWT, PSNR, MSE.

I. INTRODUCTION

Steganography is the art of hiding secret message such a way that only the intended receipient will receive the message. It is derived from the greek word stegano meaning covered and graphy means writing. It is similar to cryptography only difference being the existence of data in cryptography. In steganography we will never feel the existence of data unless the stego is distorted. So our method is to develop a method which best suits the cover. The cover means the carrier where we are hiding the message. It can be hidden inside images, audios and videos.

A typical steganographic system comprises of a stego system encoder that accepts the cover image, the message to be hidden and the optional key to generate the stego image that is identical to cover image as per the human visual systems (HVS)

Two steganographic technique exist, mainly spatial domain technique and transform domain technique. Spatial domain technique includes the least significant bit technique and transform domain technique include the Discrete Cosine transform. Spatial domain technique has the highest embedding capacity compared to the spatial domain method. But it is more prone to attacks so for a secure communication we are going for the transform domain technique.

II. LEAST BIT SIGNIFICANT TECHNIQUE

Least significant Bit method (LSB) is one of the simplest and greatly used method in steganography. Here the least bit is interchanged with a single bit of secret image. Here the message is stored in the LSB of each pixel value of cover image. Suppose we want to encode the letter A (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.

01011101 11010000 00011100 10101100
11100111 10000111 01101011 11100011

becomes

01011100 11010001 00011100 10101100
11100110 10000110 01101010 11100011

LSB Algorithm
Step1:Read the cover image and the secret message.
Step2: Convert the secret message to binary or bit stream.
Step3:Calculate the lsb operation on cover image to replace lsb of cover image with secret message.
Step 4:Write the stego image.

LSB technique is very simple and has high embedding capacity but is more prone to attacks.

III. DISCRETE COSINE TRANSFORM

The secret data within the cover image is transformed into cosine transform using Discrete Cosine Transform (DCT). A cover image represented as image representation is transformed into a frequency representation. The DCT transforms a cover image by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each. So even a slight modification in any one the pixel will affect the 64 image pixels in that block. If C(x,y) represents the cover image with x =12,.....M and y=1,2,....N. So the cover image is of MxN pixel which is divide into 8x8 blocks. In this 8x8 block DCT is performed on the (MxN/64) blocks.

The forward DCT is given by the following formula.

$$F(u,v) = C(u)\,C(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} Cos\left(\frac{(2x+1)M\pi}{2N}\right) Cos\left(\frac{(2x+1)M\pi}{2N}\right) f(x,y)$$

(1)

And inverse DCT is

$$f(x,y) - \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} C(u)\,C(v)F(u,v)Cos\left(\frac{(2x+1)M\pi}{2N}\right) Cos\left(\frac{(2x+1)M\pi}{2N}\right)$$

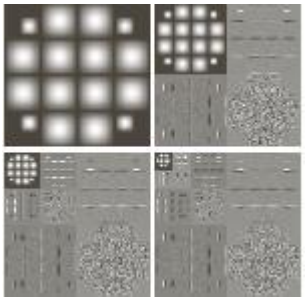
(2)

The embedding capacity is very low but is less prone to attacks

DCT Algorithm
Step1:Read the cover image and the secret message or image to hide
Step2:Convert the message into binary bit stream
Step3:Transform the cover image into discrete cosine transform using dct
Step4 :Embedding followed by inverse DCT.
Step5:Write the stego image.

IV.DISCRETE WAVELET TRANSFORM

Discrete wavelet transform is also used in the steganography. A Wavelet is a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena, A wavelet transform decomposes the signal into basis function.These basis functions are called wavelets.. In Wavelet transform, the original signal is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or bi-orthogonal scalar or multiwavelets. The wavelet convert an carrier into series of wavelet packets than pixel blocks. The 2-D DWT leads to a decomposition of approximation coefficients at level *j* in four components which are, the approximation at level *j+1*, and the details in three orientations (horizontal, vertical, and diagonal). In Wavelet transform, the original signal is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or bi-orthogonal scalar or multiwavelets.A 2-D image can be decomposed using a wavelet as shown below



Haar is the simplest of all the wavelets and it is related to a mathematical operation called Haar transform.It also decomposes the signal into sub levels.

The embedding capacity is more compared to the discrete cosine transform technique and minimizes attack.

DWT Algorithm

Step1:Read the cover image and the secret message or image to hide
Step2:Convert the message into binary bit stream
Step3:Transform the cover image into discrete wavelet transform using DWT2
Step4 :Embedding the secret message
Step5:Take the inverseDWT.
Step6:Write the stego image

V.PEROFORMANCE MATRICES

Performance of the above three techniques are compared using the Mean square error, Peak signal to noise ratio and structural content.

I.Mean Square Error

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image.

Mean Square Error=sum(sum(error)))^2/size(original image) *(3)*

II.PSNR

To compute the PSNR, the block first calculates the mean-squared error using the following equation.Then the block computes the PSNR using the following equation:

$$PSNR=10*\log_{10}(255*255/\text{Mean Square Error}) \quad (4)$$

III.Structural Content

To compute the structural content(SC) is calculated using the formula given below:

SC=sum(sum(original image))/sum(sum(distorted image)) *(5)*

VI.RESULTS AND DISCUSSIONS

In this paper the three data hiding techniques was analysed And compared the results below. .The number of characters used to hide is 337.Similarly the number of characters used to hide the text message can be increased subsequently or decresed.The PSNR,Mean Square Error and Structural Content Varies Accordingly.Computation time is also calculated for the above three methods

Table 1:PSNR Based Comparison For Hiding A Text

IMAGE	LSB Method	DCT Method	DWT Method
Baboon	50.490	33.4520	43.2700
Lena	50.5369	28.0260	44.6090

Table2 :Mean Square Error Comparison For Hiding A Text

IMAGE	LSB Method	DCT Method	DWTMethod
Baboon	0.56	29.3683	3.0625
Lena	0.5886	35.66	2.25

Table3 :Structural Content Comparison For Hiding A Text

IMAGE	LSB Method	DCT Method	DWTMethod
Baboon	1	0.2597	0.0456
Lena	1	0.0096	0.0098

Table4 : Computation Time(in seconds) Comparison For Hiding A Text

IMAGE	LSB Method	DCT Method	DWTMethod
Baboon	0.006437	3.665686	0.898871
Lena	0.006377	3.716906	0.88597

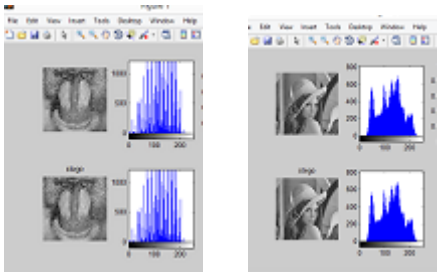


Figure1:Test Result Of (a) Baboon (b) lenaHiding Text Message based on LSBmethod

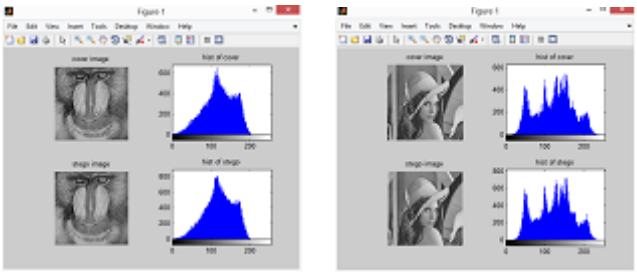


Figure2:Test Result Of (a) Baboon (b) lena Hiding Text Message based on DCT method

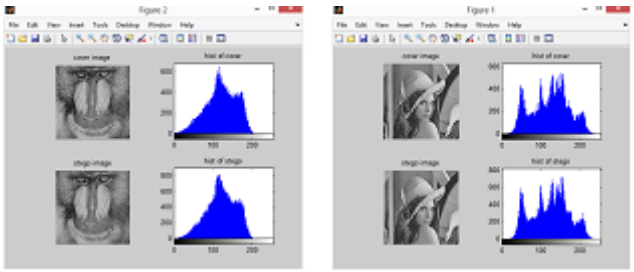


Figure3:Test Result Of (a) Baboon (b) lena Hiding Text Message based on DWT method

VII.CONCLUSION

In this paper the basic steganographic techniques are compared. The DWT technique gave the best PSNR compared to DCT. This technique is less prone to attacks.LSB gives the best PSNR value but is highly prone to attacks. The computation time is also compared along with the structural index , and mean square error. Computation time is high for DCT method and less for LSB.DWT takes less time compared to DCT.

REFERENCES

[1] Ratnakirti Roy1, Suvamoy Changder1, Anirban Sarkar1, Narayan C Debnath2**,** "Evaluating Image Steganography Techniques: Future Research Challenges" IEEE transactions 2013

[2] R. Amritharajan, R. Akila, P. Deepikachowdavarapu, "A ComparativeAnalysis of Image Steganography", International Journal of Computer Applications, Vol. 2, No.3, pp. 41-47, 2010

[3] Anjali A. Shejul, Umesh L. Kulkarni," A Secure Skin Tonebased Steganograph Using Wavelet Transform"International Journal Of computer theory and engineering,Vol 3, No.1, pp. 16-22,February,2011.

[4] N. Lavanya , V.Manjula, N.V. Krishna Rao," Robust and Secure Data Hiding in Image UsingBiometric Technique, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5133 - 51

[5] Feno Heriniaina Rabevohitra and Jun Sang"Using PSO Algorithm for simple LSB Substitution Based Steganography Scheme in DCT Transformation Domain"@Springer-Verlag Berlin Heidelberg 2011,vol pp.212-220,2011

[6] Santi P. Maity and Malay K. Kundu, "Genetic algorithmsfor optimality of data hiding in digital images" Publishedonline: 31 May 2008© Springer-Verlag 2008

[7] Emad Elbeltagi, Tarek Hegazy, Donald Grierson, "Comparison among five evolutionary-based optimization algorithms ", @ science direct Advanced Engineering Informatics 19 (2005) 43–53